

Dr inż. Witold SKOMRA

Rządowe Centrum Bezpieczeństwa

Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego

Nowe wyzwania

Przyzwyczailiśmy się, że słowo zagrożenie czy kataklizm kojarzy się głównie z czynnikami naturalnymi (powódzie, wichury, klęski żywiołowe) lub zdarzeniami o charakterze militarnym (wojny, kryzysy polityczno-militarne). Tymczasem wraz z rozwojem technologicznym następuje proces stopniowego uzależniania społeczeństwa od zdobyczy cywilizacyjnych, w tym od infrastruktury technicznej. Uzależnienie prowadzące niekiedy do ubezwłasnowolnienia ludzi w przypadku jej awarii. Występuje przy tym sprzężenie zwrotne. Wprowadzenie infrastruktury zapewniającej wodę, ciepło, energię elektryczną itd., doprowadza w krótkim czasie do podwyższenia poziomu wrażliwości społecznej, gdyż przeciętny obywatel przestaje zaopatrywać się w niezbędne środki w sposób indywidualny (zaprzestaje się budowy indywidualnych ujęć wody, niezależnych kotłowni itp.). Równocześnie pojawiają się urządzenia, a nawet całe ich systemy, bez których tak życie pojedynczych osób, jak i funkcjonowanie społeczeństw jest znacznie utrudnione. W efekcie, społeczeństwa krajów bardziej rozwiniętych są daleko bardziej narażone na uszkodzenie danego rodzaju infrastruktury technicznej niż społeczeństwa krajów słabo rozwiniętych. Taka infrastruktura zyskała nazwę infrastruktury krytycznej, w skrócie IK. Dodatkowym czynnikiem generującym zagrożenia są wzajemne zależności między różnymi rodzajami infrastruktury. Doskonałym przykładem to ilustrującym jest rola, jaką wśród różnych rodzajów IK odgrywają systemy zaopatrzenia w energię elektryczną. Telekomunikacja, transport, bankowość, to jedynie przykłady ważniejszych systemów uzależnionych od dostaw energii elektrycznej. Jej zanik, to nie tylko trudności komunikacyjne czy brak wody pitnej. Konieczność błyskawicznego uwolnienia tysięcy ludzi uwięzionych w wagonach metra i windach oraz zapewnienie zaopatrzenia w wodę pitną całych aglomeracji, to tylko część z

zadań, jakie w takich sytuacjach spoczywają na służbach ratowniczych i administracji publicznej. Trzeba jeszcze zapewnić regulację ruchu drogowego, utrzymać porządek publiczny i przede wszystkim zapewnić możliwość dokonywania zakupów leków i podstawowych artykułów żywnościowych w sytuacji załamania się bezgotówkowych systemów transakcyjnych (przecież współczesny pieniądz coraz częściej ma postać elektroniczną, a nie fizyczną). Z drugiej strony system zaopatrzenia w energię elektryczną, na przykładzie Polski, sam jest silnie uzależniony zarówno od transportu surowców niezbędnych do produkcji energii, jak i od telekomunikacji, bez której zarządzanie pracą systemu wydaje się niemożliwe (systemy sterowania i nadzoru).

Rozległa awaria systemu elektroenergetycznego lub jego części wraz ze społecznymi i gospodarczymi skutkami zaniku napięcia nosi nazwę „Blackout”. Oto przykłady takich wydarzeń: 14 sierpnia 2003 północno-wschodnia Ameryka od Ottawy i Toronto po Nowy Jork (łącznie 50 mln mieszkańców), 23.08.2003 Finlandia, 28.08.2003 Anglia, 2.10.2003 Czechy, 28.09.2003 część Francji, Szwajcarii i całe Włochy (największa jak dotąd katastrofa tego typu w Europie), 8.04.2008 Szczecin, 15.01.2010 część województw śląskiego, małopolskiego i świętokrzyskiego. Blackout, poza wymienionymi powyżej trudnościami w funkcjonowaniu społeczeństwa, to niestety także okazja do zamieszek i rabunku, poczynając od grabieży sklepów (chleb, woda, soki i baterie do latarek stają się natychmiast towarami strategicznymi) po atakowanie banków (karty kredytowe tracą znaczenie skoro nie działają bankomaty). Obawy te nie są bezpodstawne. W lipcu 1997 r. podczas zaniku prądu w Nowym Jorku obrabowano 11 tysięcy sklepów. Doszło do zamieszek ulicznych, zaś policja na wiele godzin utraciła kontrolę nad miastem¹.

To jedynie przykład do czego może doprowadzić dysfunkcja tylko jednego z coraz liczniejszych systemów w jakie łączy się infrastruktura techniczna. Jak więc widać, zdobycze cywilizacji, od których zależy komfort życia społeczeństwa, tworzą jednocześnie tzw.

¹ P. Gniadek, *Blackout*, Gazeta Południowego Koncernu Energetycznego SA "Koncern", październik 2003.

sprzyjające okoliczności² i warunki do powstania zakłóceń, a nawet potęgowania ich następstw. J. Marczak wymienia następujące cechy tego środowiska³:

- zagęszczenie ludności (budynki, wysokie, środki masowej komunikacji);
- uzależnienie warunków bytowych ludności oraz funkcjonowania transportu i gospodarki od dostaw energii elektrycznej, gazu, wody, paliwa, żywności itd.;
- rozbudowana infrastruktura krytyczna, którą stanowią budynki władz, centra łączności, centra finansowe, węzły komunikacyjne, mosty, ujęcia wody, elektrownie, stacje radiowo- telewizyjne itp.;
- istnienie potencjalnych źródeł zagrożeń takich jak składy TŚP (toksycznych środków przemysłowych), składów i rurociągów paliwa, lasów, dróg kołowych i kolejowych o dużej intensywności ruchu;
- niska świadomość zagrożonej ludności oraz słabe przygotowanie władz, społeczeństwa, infrastruktury do reagowania kryzysowego;
- ograniczona możliwość, czy w ogóle brak możliwości wsparcia wojskowego władz i społeczeństwa.

Przytoczony przykład wymaga pewnej korekty wynikającej z postępującego procesu badawczego. Po pierwsze nie każdy budynek, most czy droga jest elementem infrastruktury krytycznej. Po drugie to nie las, zakład czy zbiornik stanowi zagrożenie, a raczej awaria, czy pożar. Naukowcy zajmujący się infrastrukturą krytyczną koncentrują się obecnie nie tyle na obiektach czy urządzeniach, co raczej na usługach czy funkcjach jakie infrastrukturą dostarcza obywatelom. Dlatego bazując na wskazanych okolicznościach można sformułować nieco szersze pojęcie a mianowicie podatność⁴ społeczeństwa na zagrożenia i ich skutki. Czynnikiem wzmagającym tę podatność są:

- zagęszczenie ludności (przemieszczenie ludności do miast i tworzenie wielkich aglomeracji oraz dużych skupisk wysokich budynków), w tym czasowa

² W oryginale z języka angielskiego: environment favorable - środowisko sprzyjające.

³ J. Marczak, Podstawowe założenia połączonych działań OT i UP w sytuacjach kryzysowych, [w:] J. Marczak (kier. nauk.), Przygotowanie i koordynacja połączonych działań obrony terytorialnej i układu pozamilitarnego w sytuacjach kryzysowych „Koordynacja” – część druga, AON, Warszawa 2003, s. 12.

⁴ podatność - cechy charakterystyczne zasobów, infrastruktury, systemów, społeczeństwa lub procesów, które czynią je wrażliwymi na zniszczenie, zakłócenie funkcjonowania, zmniejszenie potencjału lub efektywności działania oraz niewłaściwe wykorzystanie, w drodze wystąpienia klęsk żywiołowych, intencjonalnej działalności człowieka, awarii technicznych lub innych szkodliwych działań. Podatność określa jednocześnie trudności (wyzwania) w ochronie zasobów, infrastruktury, systemów, społeczeństwa lub procesów.

koncentracja w określonych obszarach i miejscach (biurowce, środki masowej komunikacji w godzinach pracy, miejsca imprez sportowych czy centra handlowe w okresach wzmożonych zakupów);

- uzależnienie ludności od dostaw usług, podnoszących jakość warunków bytowych (bieżąca woda, żywność, energia elektryczna, paliwa, łączność, komunikacja, transport itp.);
- rozbudowana infrastruktura, od której uzależnione są dostawy ww. usług;
- występowanie, infrastruktury która jednocześnie może stanowić źródło zagrożeń dla społeczeństwa (np. zakłady o dużym ryzyku wystąpienia poważnej awarii przemysłowej);
- wykorzystanie cyberprzestrzeni⁵ w gospodarce, administracji oraz codziennym życiu obywateli;
- niska świadomość zagrożonej ludności oraz nieadekwatne przygotowanie władz, społeczeństwa, infrastruktury do reagowania kryzysowego;
- niedostateczne i nieadekwatne wyposażenie służb odpowiedzialnych za reagowanie kryzysowe, w tym ograniczona możliwość, czy w ogóle brak możliwości ich wsparcia w przypadku wyczerpania posiadanych sił i środków.

Na istnienie tych nowych, cywilizacyjnych źródeł zagrożeń zwrócono (choć ogólnie) uwagę w „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej”. Zgodnie z nią „pojawienie się nowych form zagrożeń, w szczególności zagrożeń asymetrycznych oraz związanych z rozwojem cywilizacyjnym, napięciami politycznymi i społecznymi, wymusza bardziej zdecydowane poszukiwanie nowych rozwiązań celem sprawniejszej realizacji zadań z zakresu zarządzania kryzysowego i ochrony ludności, w tym obrony cywilnej”⁶.

Jak widać w omawianym obszarze całościowe podejście do sytuacji kryzysowych obejmuje jednocześnie podnoszenia odporności elementów infrastruktury i obniżanie stopnia wrażliwości społeczności potencjalnie dotkniętej skutkami braku niezbędnej usługi czy funkcji.

⁵ Cyberprzestrzeń - cyfrowa przestrzeń komunikacyjna tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniem pomiędzy nimi oraz relacjami z użytkownikami.

⁶ Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, <http://www.bbn.gov.pl/portal.php?serwis=pl&dzial=475&id=1144&search=530>, s.28.

Całościowe podejście do zarządzania w sytuacjach kryzysowych na przykładzie zapobiegania poważnym awariom przemysłowym.

Takie podejście wcale nie jest zupełnym novum. Jego elementy można dostrzec w rozwiązaniach wprowadzonych dyrektywą Rady Unii Europejskiej 96/82/WE (SEVESO II) z 9 grudnia 1996 r. w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi (16 grudnia 2003 r. została wydana poprawka/uzupełnienie w postaci Dyrektywy 2003/105/WE). Implementacją do polskiego systemu prawnego omawianej dyrektywy jest ustawa Prawo ochrony środowiska⁷. I tak zgodnie z tą ustawą ochrona środowiska przed poważną awarią oznacza jednocześnie zapobieganie zdarzeniom mogącym powodować awarię oraz ograniczanie jej skutków dla ludzi i środowiska. W efekcie podmiotami odpowiedzialnymi za tak rozumianą ochronę środowiska są nie tylko podmioty prowadzące zakład czy dokonujące przewozu substancji niebezpiecznych, ale również organy administracji są publicznej. Podstawowym narzędziem do przygotowania przyszłych działań od strony podmiotu jest program zapobiegania poważnym awariom przemysłowym, w którym przedstawia się system bezpieczeństwa gwarantujący ochronę ludzi i środowiska.

Program zapobiegania awariom powinien zawierać w szczególności:

- 1) określenie prawdopodobieństwa zagrożenia awarią przemysłową;
- 2) zasady zapobiegania oraz zwalczania skutków awarii przemysłowej przewidywane do wprowadzenia;
- 3) określenie sposobów ograniczenia skutków awarii przemysłowej dla ludzi i środowiska w przypadku jej zaistnienia;
- 4) określenie częstotliwości przeprowadzania analiz programu zapobiegania awariom w celu oceny jego aktualności i skuteczności.

Dla przygotowania działań po wystąpieniu awarii opracowywane są wewnętrzny i zewnętrzny plan operacyjno-ratowniczy.

⁷ Ustawa z dnia 27 kwietnia 2001 r., Prawo ochrony środowiska, Dz.U. z 2008, nr 25, poz.150.

Plany operacyjno-ratownicze zawierają w szczególności:

- 1) zakładane działania służące ograniczeniu skutków awarii przemysłowej dla ludzi i środowiska;
- 2) propozycje metod i środków służących ochronie ludzi i środowiska przed skutkami awarii przemysłowej;
- 3) informację o występujących zagrożeniach, podjętych środkach zapobiegawczych i o działaniach, które będą podjęte w przypadku wystąpienia awarii przemysłowej, przedstawianą społeczeństwu i właściwym organom Państwowej Straży Pożarnej, wojewodzie, wojewódzkiemu inspektorowi ochrony środowiska, regionalnemu dyrektorowi ochrony środowiska, staroście, wójtowi, burmistrzowi lub prezydentowi miasta;

W przypadku gdy przewiduje się oddziaływanie skutków awarii poza terenem zakładu - zewnętrzny plan operacyjno-ratowniczy sporządza komendant wojewódzki Państwowej Straży Pożarnej. W trakcie jego opracowywania Komendant zapewnia możliwość udziału społeczeństwa, którego postanowienia planu dotyczą. Jednym z istotnych elementów informowania społeczeństwa o możliwych zagrożeniach jest podawanie do publicznej wiadomości rejestru substancji niebezpiecznych znajdujących się w poszczególnych zakładach. Ponadto do zadań komendanta należy opracowywanie i publikacja instrukcji o postępowaniu mieszkańców na wypadek wystąpienia awarii. Szczegółowe wymagania dla planów wynikają z rozporządzenia ministra gospodarki, pracy i polityki społecznej⁸. Zgodnie z nim plan zawiera:

- 1) wskazanie osób upoważnionych do uruchamiania procedur ratowniczych, osoby kierującej działaniami ratowniczymi oraz nadzorującej i koordynującej działania w zakresie usuwania skutków awarii;
- 2) zbiorczy wykaz sił i środków służb ratowniczych oraz służb wspomagających, przewidzianych do prowadzenia działań ratowniczych i usuwania skutków awarii;

⁸ Rozporządzenie ministra gospodarki, pracy i polityki społecznej dnia 17 lipca 2003 r., w sprawie wymagań, jakim powinny odpowiadać plany operacyjno-ratownicze (Dz. U. z 2003 r. nr 131, poz.1219).

- 3) opis systemu przedstawiania społeczeństwu informacji o występujących zagrożeniach związanych z działalnością zakładu, podjętych środkach zapobiegawczych i działaniach, które będą podejmowane w razie wystąpienia awarii;
- 4) procedury powiadamiania ludności i właściwych organów administracji o zagrożeniu awarią lub jej wystąpieniu;
- 5) procedury dotyczące ewakuacji ludności;
- 6) procedury udzielenia pomocy medycznej osobom poszkodowanym;
- 7) procedury postępowania związane z możliwością wystąpienia transgranicznych skutków awarii;
- 8) procedury postępowania poawaryjnego;
- 9) określenie sposobów zabezpieczenia logistycznego działań ratowniczych;
- 10) inne niezbędne informacje wynikające ze specyfiki zagrożenia oraz lokalnych uwarunkowań, w szczególności:
 - a. procedury powiadamiania właściwych organów o możliwości wystąpienia lub wystąpieniu poważnej awarii,
 - b. informacje dotyczące działań podejmowanych przez właściwe organy w celu ograniczenia skutków awarii dla ludzi i środowiska.

Zawarte w planach szczegółowe procedury dotyczące ewakuacji ludności obejmują:

- 1) określenie kolejności ewakuacji, z uwzględnieniem osób wymagających specjalnych środków podczas jej przeprowadzania, w szczególności dotyczy to dzieci, pacjentów szpitali, pensjonariuszy domów pomocy społecznej oraz innych osób zamieszkałych w obiektach użyteczności publicznej i zamieszkania zbiorowego;
- 2) sposoby prowadzenia ewakuacji i zabezpieczenia potrzeb socjalnych ewakuowanej ludności;

- 3) wykaz instytucji i służb odpowiedzialnych za przeprowadzenie ewakuacji, zabezpieczenie potrzeb socjalnych i pomocy psychologicznej ewakuowanej ludności, wraz z wyszczególnieniem realizowanych przez nie zadań;
- 4) sposoby alarmowania podmiotów odpowiedzialnych za przyjęcie oraz ochronę ewakuowanej ludności;
- 5) sposoby zabezpieczenia mienia ewakuowanej ludności.

Wśród pozostałych elementów planowania są jeszcze uwzględnione m.in. procedury udzielania pomocy medycznej osobom poszkodowanym w tym zasady przeprowadzania dekontaminacji tych osób.

Cennym rozwiązaniem zastosowanym przy ocenie zagrożeń wynikających z działalności omawianych zakładów jest pojęcie efektu domina. I tak komendant wojewódzki Państwowej Straży Pożarnej może ustalić, w drodze decyzji, grupy zakładów o zwiększonym ryzyku lub o dużym ryzyku, których zlokalizowanie w niedużej odległości od siebie może zwiększyć prawdopodobieństwo wystąpienia awarii przemysłowej lub pogłębić jej skutki, w szczególności ze względu na skoncentrowanie posiadanych rodzajów, kategorii i ilości substancji niebezpiecznych. Wprawdzie przyjęta metodyka szacowania takiego zagrożenia sumarycznego nie może być wprost przeniesiona na zagadnienia związane z ochroną IK, ale sam fakt, że w postępowaniu administracyjnym dotyczącym jednego podmiotu można wykorzystać analizę jego otoczenia jest cennym rozwiązaniem do ewentualnego wykorzystania.

Ochrona ludności przed skutkami awarii infrastruktury, w tym infrastruktury krytycznej

Przedstawiona powyżej informacja o funkcjonowaniu dyrektywy Seveso II ma nie tylko charakter poznawczy. Instalacje, obiekty czy urządzenia niektórych zakładów znajdujących się na omawianych wykazach może zostać uznana za IK. W takim przypadku

niecelowym byłoby dublowanie rozwiązań, które już zostały wdrożone. Ponadto warto opierać się na rozwiązaniach, które już zostały wdrożone i przetestowane. Ochrona ludności cywilnej przed skutkami awarii IK według obecnego stanu prawnego nie może być zorganizowana jakościowo na takim poziomie jak w omówionym przykładzie. Po pierwsze trwa dopiero proces wyłaniania elementów IK. Żaden ośrodek naukowy nie pokusił się jeszcze o rzetelną analizę zakresu oddziaływania dysfunkcji IK na poziom bezpieczeństwa i jakość życia obywateli. Sporą trudnością w planowaniu zadań będzie niejawność tak kryteriów wyłaniania IK, jak i wykazu krajowej i europejskiej IK. W efekcie ani nie znamy wszystkich możliwych narzędzi jakie powinny być w takich sytuacjach zastosowane ani nie ma odpowiedniej obudowy prawnej. Jednak wydaje się, że możliwe oddziaływania spowodowane uszkodzeniem IK będą jedynie zwielokrotnieniem skutków jakie może wywołać awaria infrastruktury lokalnej. Poza skalą różne będą jedynie sposoby wsparcia właściciela czy operatora infrastruktury oraz zakres i sposoby wsparcia działań władz na niższych szczeblach administracyjnych. Właśnie ta konieczność współdziałania, współpracy i wzajemnego wsparcia jest cechą charakterystyczną dla skutecznego zarządzania w sytuacjach kryzysowych. Stąd rozwiązania już przyjęte w systemie zarządzania kryzysowego mogą i powinny być zastosowane celem minimalizacji, choćby tych już rozpoznanych, skutków awarii infrastruktury w tym Infrastruktury krytycznej.

Na początek należy zauważyć, że to co dla szczebla centralnego jest jedynie lokalną drogą czy mostem, dla danej społeczności może być infrastrukturą krytyczną w takim rozumieniu, że jej brak może zahamować rozwój lub wręcz zagrażać życiu i zdrowiu ze względu na utrudniony dostęp do służb ratowniczych czy pomocy medycznej. Fakt, że zarządzanie kryzysowe opiera się na jednolitej metodyce planowania obejmującej wszystkie poziomy administracji publicznej w połączeniu z planowaniem branżowym w ramach poszczególnych działów administracji nie oznacza, że należy pomijać te pozornie mało istotne źródła zagrożeń. Wręcz przeciwnie, plany zarządzania kryzysowego obejmują m.in. „organizację ochrony przed zagrożeniami charakterystycznymi dla danego obszaru”. Aby jednak określić te zagrożenia wszystkie plany opierają się na analizie możliwych zagrożeń. Do zobrazowania zagrożeń powodowanych przez uszkodzenia infrastruktury lokalnej pomocne będą mapy ryzyka. Mapy te są rozumiane nie tylko jako zobrazowanie graficzne, ale również opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę. Tak więc na każdym szczeblu organ zarządzania

kryzysowego powinien uwzględnić nie tylko możliwość uszkodzenia infrastruktury lokalnej, ale również przeanalizować jej skutki.

Na tak sporządzony materiał wyjściowy należy nałożyć dane odnośnie oddziaływania krajowej IK. Pierwszym źródłem informacji o tych oddziaływaniach są kryteria przekrojowe do wyłaniania IK, gdzie wprost podano ilość osób jakie trzeba będzie ewakuować czy np. ilość użytkowników, którzy zostaną pozbawieni usługi np. zaopatrzenia w wodę. Wszystkie te informacje będą dostępne dla szczebla krajowego i wojewódzkiego. I od tych szczebli zarządzania kryzysowego należy rozpocząć proces włączania skutków awarii IK do planów zarządzania kryzysowego.

Pierwszym krokiem będzie wydanie wytycznych do sporządzania wojewódzkich planów zarządzania kryzysowego. Wytyczne będą głównie oparte o wnioski z Raportu w sprawie zagrożeń bezpieczeństwa narodowego, ale nic nie stoi na przeszkodzie by je rozwinąć poprzez wskazanie wprost zadań do wykonania wynikających z zagrożeń o charakterze ponadwojewódzkim. W tym zakresie źródłem informacji będą plany zarządzania kryzysowego poszczególnych resortów i postanowienia Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK). Tak więc w wytycznych powinny się znaleźć m.in. takie informacje jak skala przewidywanych ewakuacji, zakres niezbędnej pomocy medycznej w sytuacjach kryzysowej, zakres możliwego wsparcia przy pomocy Sił Zbrojnych itp.

W drugim kroku, po uzupełnieniu o zagrożenia charakterystyczne dla danego województwa, wojewoda wydaje zalecenia do sporządzenia powiatowych planów zarządzania kryzysowego (art.14, ust.2. pkt 2 ppkt a ustawy o ZK). Wprawdzie słowo zalecenia sugeruje niewładczą formę oddziaływania, ale ponieważ wojewoda zatwierdza plan powiatowy to w efekcie zalecenia będą miały dla wykonawców w praktyce charakter wiążący. Poza elementami składowymi planu wytyczne powinny zawierać zadania do wykonania z zakresu ochrony ludności wynikające ze wszystkich potencjalnych zagrożeń, w tym oczywiście ze spodziewanych skutków awarii IK. Powinny również obejmować nie tylko zadania własne szczebla powiatowego, ale również zadania własne szczebla gminnego. Szczególny nacisk należy położyć na kwestie związane z zapewnieniem podstawowych warunków przetrwania dla ewakuowanej ludności, gdyż zagadnienie to jest zadaniem własnym gminy i wyższe szczeble mogą jedynie wspomagać gminę w jego realizacji. Z kolei poszczególne gminy, ze

względu na ograniczenia w dostępie do informacji niejawnych, nie muszą posiadać pełnej wiedzy np. co do skali spodziewanej ewakuacji.

Podobny mechanizm funkcjonuje na szczeblu powiatu. Mianowicie starosta wydaje organom gminy zalecenia do gminnego planu zarządzania kryzysowego. Dokonuje również jego zatwierdzenia. Bazując zatem na zaleceniach jakie sam otrzymał od wojewody może skoordynować przygotowania samorządu do działań po awarii IK. Ten szczebel należy uznać za kluczowy dla osiągnięcia właściwego poziomu bezpieczeństwa obywateli przy omawianych zagrożeniach. W przeciwieństwie do administracji rządowej szczebel samorządowy ma do dyspozycji nieco odmienne metody współdziałania we wszystkich dziedzinach. Takim narzędziem umożliwiającym współpracę starosty z wójtami jest możliwość wzajemnego udzielania sobie pomocy⁹. Tą drogą samorządy mogą obniżyć koszty działań (zamiast przygotowywać przykładowo po 3 tys. miejsc ewakuacyjnych w każdej gminie, wystarczy przygotować ich 1000, a jednocześnie zapewnić sobie możliwość użycia miejsc przygotowanych w gminach sąsiednich). Dodatkowo mogą wprowadzić wspólny obieg informacji o zagrożeniach, posiadanych zapasach i podejmowanych działaniach. Wsparciem tych działań dla starosty może być prawo do żądania informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie¹⁰.

Przedstawiony mechanizm przekazywania informacji o zagrożeniach i jego potencjalnych skutkach oraz wzajemne wsparcie w fazie reagowania nie są jedynymi zadaniami jakie ustawodawca nałożył na organy zarządzania kryzysowego. Należy jeszcze uwzględnić konieczność przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. Wprawdzie obowiązki te nałożono w związku z krajową IK, ale nic nie stoi na przeszkodzie by to samo podejście zastosowano wobec infrastruktury lokalnej w ramach realizacji zadań własnych poszczególnych rodzajów samorządu terytorialnego. Tym bardziej, że uszkodzenia dróg, mostów wałów przeciwpowodziowych itp. często powodują skutki dalece wykraczające poza teren jednej jednostki administracyjnej.

⁹ Ustawa z dnia 5 czerwca 1998r., *o samorządzie powiatowym*, (Dz.U. 2001r., nr 142, poz. 1592 t.j. z późn. zm., art. 7a. oraz ustawa z dnia 8 marca 1990r., *o samorządzie gminnym*, (Dz.U. 2001r., nr 142, poz. 1591, t.j. z późn. zm., art. 10, ust.2.

¹⁰ Ustawa z dnia 26 kwietnia 2007r., *o zarządzaniu kryzysowym*, (Dz.U. nr 89, poz. 590, art. 20a.

Istnieje też obszar który został dość specyficznie zdefiniowany w ustawie o zarządzaniu kryzysowym. Jest to mianowicie etap odbudowy IK. Generalnie szybkie odtworzenie IK lub przywrócenie jej funkcjonalności jest przede wszystkim obowiązkiem jej właścicieli oraz posiadaczy samoistnych i zależnych. Natomiast rola administracji publicznej sprowadza się jedynie do stworzenia dogodnych warunków do tego procesu (o ile sama nie jest ona właścicielem IK). Zagadnienie wsparcie etapu odbudowy jest niezwykle drażliwym. Znaczna część IK nie jest obecnie własnością administracji publicznej. Pomoc w tej dziedzinie będzie zatem kierowana do podmiotów gospodarczych. Może to budzić obawy co do legalności wspierania działalności gospodarczej z pieniędzy podatnika. Z drugiej jednak strony świadomość, że przedłużający się okres dysfunkcji IK doprowadzić może to zagrożenia życia i zdrowia obywateli, wymusi na rządzących udzielenie takiego wsparcia i to nawet w sytuacji braku odpowiednich regulacji prawnych. Już dzisiaj ustawa o zarządzaniu kryzysowym wprowadziła odbudowę IK jako jeden z elementów zarządzania. Ponadto opiniowanie potrzeb w zakresie odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru jest jednym z zadań Rządowego Zespołu Zarządzania Kryzysowego. W efekcie po pierwszym okresie tworzenia NPOIK należy spodziewać się powstania kolejnego programu, czy strategii w której będą proponowane inwestycje mające obniżyć poziom wrażliwości społeczeństwa na uszkodzenia IK. Należy również oczekiwać, że rozszerzeniu ulegnie zakres działania realizowany dotychczas przez Biuro do Spraw Usuwania Skutków Klęsk Żywiolowych. Dotychczasowa praktyka wspierania finansowego administracji rządowej i samorządowej celem realizacji jej zadań ustawowych w sytuacji wyczerpania środków finansowych, powinna zostać rozszerzona. W szczególności poprzez wsparcie działań samych obywateli (np. dopłaty do ubezpieczeń klęskowych nad którymi już trwają prace koncepcyjne) oraz na wsparcie operatorów IK. W tym drugim przypadku możliwym jest udzielenie gwarancji rządowych na kredyty zaciągane celem usunięcia awarii czy uruchomienie rezerw strategicznych .

Jak więc widać, pomimo że na dzień dzisiejszy nie istnieją specjalne rozwiązania prawne z zakresu ochrony ludności przed skutkami awarii IK, to na bazie ogólnych zadań organów zarządzania kryzysowego można już wdrażać niektóre rozwiązania z tego zakresu. Warunkiem powodzenia jest zapewnienie korelacji pomiędzy już zebranymi informacjami o oddziaływaniu IK, a dokumentami wyjściowymi do opracowania planów zarządzania kryzysowego. Dodatkowo, aby osiągnąć efekt synergii, zamiast metody nakazowej w

kontaktach z organami samorządowymi, należy zainicjować metodę wspólnej realizacji zadań własnych przy technicznym i finansowym wsparciu administracji rządowej.

Podsumowanie

1. Pojęcie infrastruktury krytycznej powinno być ściśle powiązane ze szczeblami administracji publicznej. Jednocześnie niższe szczeble powinny posiadać wiedzę o istnieniu IK i to nawet wówczas, gdy dany system nie oddziałuje bezpośrednio na daną społeczność.
2. Wyłanianie IK musi być oparte m.in. o efekty społeczne i gospodarcze wywoływane przez dysfunkcję danego systemu.
3. Ochrona ludności przez skutkami dysfunkcji IK musi obejmować jednocześnie dwa elementy:
 - a) wzrost odporności elementów IK na przewidywalne zagrożenia;
 - b) obniżanie wrażliwości społecznej na skutki spodziewanej awarii.
4. Z racji ponadlokalnych i ponadregionalnych oddziaływań IK warunkiem właściwego przygotowania się na jej ewentualne awarie jest współodpowiedzialność współdziałanie i współpraca i to zarówno w relacjach pomiędzy administracją publiczną i operatorami IK, jak i w relacjach pomiędzy poszczególnymi rodzajami i poziomami administracji publicznej.

Bibliografia

1. Ustawa z dnia 27 kwietnia 2001 r., Prawo ochrony środowiska, Dz.U. z 2008r., nr 25, poz.150.
2. Ustawa z dnia 5 czerwca 1998r, *o samorządzie powiatowym*, Dz.U. 2001r., nr 142, poz. 1592 t.j. z późn. zm.

3. Ustawa z dnia 8 marca 1990r., *o samorządzie gminnym*, Dz.U. 2001r., nr 142, poz. 1591, t.j. z późn. zm.
4. Ustawa z dnia 26 kwietnia 2007r., *o zarządzaniu kryzysowym*, (Dz.U. nr 89, poz.590).
5. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, <http://www.bbn.gov.pl/portal.php?serwis=pl&dzial=475&id=1144&search=530>
6. Rozporządzenie ministra gospodarki, pracy i polityki społecznej dnia 17 lipca 2003 r., *w sprawie wymagań, jakim powinny odpowiadać plany operacyjno-ratownicze* Dz. U. z 2003 r. nr 131, poz.1219.
7. P. Gniadek, *Blackout*, Gazeta Południowego Koncernu Energetycznego SA "Koncern", październik 2003.
8. J. Marczak, Podstawowe założenia połączonych działań OT i UP w sytuacjach kryzysowych, [w:] J. Marczak (kier. nauk.), *Przygotowanie i koordynacja połączonych działań obrony terytorialnej i układu pozamilitarnego w sytuacjach kryzysowych „Koordynacja”*– część druga, AON, Warszawa 2003.